



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

50

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/855,183	05/14/2001	Ron J. Vandergeest	10500.00.8172	8194
23418	7590	05/20/2005	EXAMINER	
VEDDER PRICE KAUFMAN & KAMMHOLZ 222 N. LASALLE STREET CHICAGO, IL 60601			HA, LEYNNA A	
			ART UNIT	PAPER NUMBER
			2135	
DATE MAILED: 05/20/2005				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/855,183

Applicant(s)

VANDERGEEST ET AL.

Examiner

LEYNNA T. HA

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 18 January 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-17 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-17 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-17 are not currently amended.
2. Claims 1-17 remains rejected under 35 U.S.C. 102(e).

This is a Final rejection because no new art is introduced.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. **Claims 1-17 are rejected under 35 U.S.C. 102(e) as being anticipated by Okomoto, et al. (US 5,944,794).**

As per claim 1:

Okomoto discloses a method for providing user authentication comprising:

(a) sending, by a first unit, user identification data to an authentication unit; **[col.18, lines 52-65 and col.19, lines 33-35 and 63-65]**

(b) using the user identification data to determine which intermediate destination unit will receive an authentication code to be used to authenticate the user; **[col.13, lines 63-67 and col.19, lines 44-48]**

(c) sending the authentication code to the determined intermediate destination unit based on the user identification data via a first secondary channel; **[col.18, lines 45-67 and col.21, lines 62-67]**

(d) re-transmitting, by the intermediate destination unit, the authentication code to the first unit via a second secondary channel in a way that is transparent to the user; **[col.20, lines 20-28 and col.21, lines 19-45]**

(e) in response to receiving the re-transmitted authentication code from the intermediate destination unit, returning the authentication code to the authentication unit; and **[col.22, lines 11-17]**

(f) authenticating the user when the returned authentication code is determined to be suitable. **[col.22, lines 18-22 and col.23, lines 1-14]**

As per claim 2:

Okomoto discusses the method of claim 1 including the step of providing selection of a third unit transparent authentication code submission scheme

and selecting the third unit transparent authentication code scheme in response to receiving selection data. **[col.23, lines 51-60 and col.24, lines 34-50]**

As per claim 3:

Okomoto discusses the method of claim 1 including the step of maintaining per user destination unit data including at least one destination unit identifier per user and wherein the step of using the user identification data to determine which destination unit will receive the authentication code includes sending the authentication code to the determined intermediate destination unit based on the stored per user destination unit identifier. **[col.21, lines 43-45 and col.22, lines 11-17]**

As per claim 4:

Okomoto discusses the method of claim 1 wherein the second secondary channel is short range channel and including the step of notifying, by the second unit, the first unit of a short range secondary channel used to receive the retransmitted authentication code from the third unit. **[col.21, lines 19-22]**

As per claim 5:

Okomoto discusses the method of claim 1 including the steps of:

prior to returning the authentication code to the authentication unit, digitally signing, by the first unit, the returned authentication code to produce

a digitally signed authentication code that was received from the determined destination unit; and **[col.14,lines 15-22]**

verifying the digitally signed authentication code as part of step (f).

[col.25, lines 12-37]

As per claim 6:

Okomoto discloses a method for providing user authentication comprising:

receiving by an intermediate unit, from an authentication unit via a first secondary channel, an authentication code for a first unit; and **[col.20, lines 20-28 and col.21, lines 19-45]**

re-transmitting, by the intermediate destination unit, the authentication code to the first unit via a second secondary channel in a way that is transparent to a user of the first unit. **[col.28, lines 8-14]**

As per claim 7:

Okomoto discusses the method of claim 6 including the step of transforming the authentication code prior to the step of re-transmitting via the second secondary channel. **[col.20, lines 20-28 and col.21, lines 19-45]**

As per claim 8:

Okomoto discloses a method for providing user authentication comprising:

sending, by a first unit, user identification data to an authentication unit; **[col.18, lines 52-65 and col.19, lines 33-35 and 63-65]**

receiving a re-transmitted authentication code that was previously sent by an authentication unit to an intermediate destination unit; and **[col.19, lines 40-47]**

in response to receiving the re-transmitted authentication code from the intermediate destination unit, returning the authentication code to the authentication unit. **[col.22, lines 11-18 and col.23, lines 12-14]**

As per claim 9:

Okomoto discusses the method of claim 8 including the step of controlling a short range receiver to receive the re-transmitted authentication code in response to receiving notification from the authentication unit and wherein returning the authentication code to the authentication unit includes returning the authentication code in a way that is transparent to the user of the first unit. **[col.22, lines 11-18]**

As per claim 10:

Okomoto discloses a storage medium comprising:
memory containing executable instructions that when executed by one or more processors, causes the one or more processors to:

send, by a first unit, user identification data to an authentication unit;

[col.18, lines 52-65 and col.19, lines 33-35 and 63-65]

use the user identification data to determine which intermediate destination unit will receive an authentication code to be used to authenticate the user; **[col.19, lines 33-47]**

send the authentication code to the determined intermediate destination unit based on the user identification data via a first secondary channel; **[col.20, lines 20-28 and col.21, lines 19-45]**

re-transmit, by the intermediate destination unit, the authentication code to the first unit via a second secondary channel in a way that is transparent to the user; **[col.18, lines 45-67 and col.19, lines 33-44]**

in response to receiving the re-transmitted authentication code from the intermediate destination unit, return the authentication code to the authentication unit; and **[col.22, lines 11-17]**

authenticate the user when the returned authentication code is determined to be suitable. **[col.22, lines 18-22 and col.23, lines 1-14]**

As per claim 11:

Okomoto discusses the storage medium of claim 10 including memory containing instructions that when executed by one or more processors, causes the one or more processors to provide selection of a third unit transparent authentication code submission scheme and selecting the third unit

transparent authentication code scheme in response to receiving selection data. **[col.23, lines 51-60 and col.24, lines 34-50]**

As per claim 12:

Okomoto discusses the storage medium of claim 10 wherein the second secondary channel is short range channel and including memory containing instructions that when executed by one or more processors, causes the one or more processors to notify, by the second unit, the first unit of a short range secondary channel used to receive the retransmitted authentication code from the third unit. **[col.21, lines 19-22 and col.25, lines 12-37]**

As per claim 13:

Okomoto discloses a system for providing user authentication comprising:

a first unit; **[col.18, lines 41-45]**

a second unit operatively coupleable to the first unit via a primary wireless channel and operatively coupleable to an authenticator; and **[col.18, lines 57-58 and col.20, lines 30-34]**

a third unit, operatively coupleable to the second unit via a wireless back channel and operatively coupleable to the first unit via a secondary short range channel, the first unit operative to send primary authentication information via the primary channel during a session to the second unit; **[FIG.15; col.18, lines 52-65 and col.19, lines 33-35 and 63-65]**

the authenticator operative to use the primary authentication information to determine which destination unit, other than the first unit, will receive an authentication code as secondary authentication information via the wireless back channel and wherein the destination unit is the third unit;
[col.19, lines 33-47]

the second unit operative to the send the authentication code on the wireless back channel to the destination unit based on the primary authentication information sent via the primary channel during the same session; **[col.22, lines 11-17]**

the destination unit operative to re-transmit the authentication code to the first unit via a second secondary channel in a way that is transparent to a user of the first unit; **[col.21, lines 19-22 and col.25, lines 12-37]**

the first unit operative to return the authentication code on the wireless primary channel to the second unit during the same session; and

the authenticator operative to authenticate the user when the returned authentication code received from the wireless primary channel is determined to be suitable. **[col.22, lines 18-22 and col.23, lines 1-14]**

As per claim 14:

Okomoto discusses the system of claim 13 wherein the authenticator maintains per user destination unit data including at least one destination unit identifier per user and sends the authentication code to the second unit for

transmission to the destination unit based on the stored per user destination unit identifier. **[col.21, lines 43-45 and col.22, lines 11-17]**

As per claim 15:

Okomoto discusses the system of claim 13 wherein the first unit includes a cryptographic engine and prior to the first unit returning the authentication code for the authenticator **[col.22, lines 11-17]**, digital signs the returned authentication code to produce a digitally signed authentication code that was received from the third unit; and **[col.25, lines 62-66]**

wherein the authenticator verifies the digitally signed authentication code as part of authenticating the user. **[col.25, lines 12-37]**

As per claim 16:

Okomoto discloses an apparatus for providing user authentication comprising:

means for receiving from an authentication unit via a first secondary channel, an authentication code for a first unit; and **[col.20, lines 19-28 and col.23, lines 1-14]**

means for re-transmitting the authentication code to the first unit via a second secondary channel in a way that is transparent to a user of the first unit. **[col.18, lines 45-67 and col.19, lines 33-44]**

Art Unit: 2135

As per claim 17:

Okomoto discusses the apparatus of claim 16 including a transformation circuit that transforms the authentication code prior to re-transmitting via the second secondary channel. **[col.20, lines 20-28 and col.21, lines 19-45]**

Response to Arguments

4. The Examiner finds the claim language broad and does not limit anymore than what is claimed. The Examiner is only required to give light the broadest reasonable interpretation for what is claimed. The Examiner maintains the rejection because Okomoto does teach a the concept of authenticating the user data wherein including a first unit, an intermediate unit, and an authentication unit on col.18-col.19. The intermediate unit can be interpreted as any unit that receives the authentication code to authenticate the user which in Okomoto may be the connection management unit or the correspondence establishing unit (col.16, lines 15-43 and col.21, lines 20-30).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

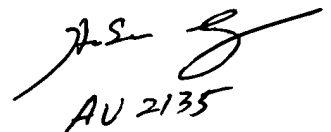
A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



AV 2135

LHA